SECTION 3
Addendum B -
Statutory and OMB Requirements Outline

Federal Regulations

1. FISMA (Federal Information Security Management Act of 2002)

The E-Government Act (Public Law 107-347) passed by the one hundred and seventh Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include:

• **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

• **Policies and procedures** that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;

• **Subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;

• **Security awareness training** to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;

• **Periodic testing and evaluation** of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;

• **A process for planning, implementing, evaluating, and documenting** remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;

• **Procedures for detecting, reporting, and responding** to security incidents; and

• **Plans and procedures to ensure continuity of operations** for information systems that support the operations and assets of the agency.

44 U.S.C. §§ 3541, 3544
§ 3541 Purpose
The purpose of FISMA is to:

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

§ 3544 Federal agency responsibilities

The head of each agency shall

(a)(1) be responsible for

(A) providing information security protections;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes.

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations assets under their control, including through;

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards for information security classifications;

(C) implementing policies and procedures to reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

(3) delegate to the agency CIO the authority to ensure compliance with the requirements imposed on the agency, including:

(A) ***CISO*** **-** designating a senior agency information security officer;

(B) ***Security Program*** **-** developing and maintaining an agencywide information security program;

(C) ***Policies*** **-** developing and maintaining information security policies, procedures, and control techniques;

(D) ***Training*** **-** training and overseeing personnel with significant responsibilities; and

(E) assisting senior agency officials concerning their responsibilities.

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements

(5) ensure **CIO reports annually** to the agency head on the effectiveness of the agency information security program

(b) implement information security program that includes

(1) ***Risk Assessment*** **-** periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency

(6) ***POA&M*** **-** a process for planning, implementing, evaluating, and documenting

remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency

(7) ***Incident Response*** **-** procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued

(c) ***Agency Reporting*** **-** each agency shall

(1) report annually on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements

(2) address the adequacy and effectiveness of information security policies, procedures, and practices

(3) report any significant deficiency in a policy, procedure, or practice identified

(d) ***Performance Plan***

(1) each agency shall include a description of (A) the time periods, and (B) the resources, including budget, staffing, and training, that are necessary to implement the program.

(2) The description shall be based on the risk assessment.

2. OMB Circular A-130

OMB A-130 establishes "security guidance" for Federal systems, issued in response to the Paperwork Reduction Act of 1980 (P.L. 104-13 and 44 U.S.C. Chapter 35, which established "a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner").

a. A minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123

b. Authorization of a system to process information. By authorizing a system, a manager accepts the risk association with it. Management authorization is based on an assessment of management, operational, and technical controls

OMB Circular A-130 Appendix III

A. Requirements

1. Purpose – establishes a minimum set of controls to be included in Federal automated information security programs
2. Definitions
3. Automated Information Security Programs. Implement policies, standards and procedures. At a minimum, agency programs shall include the following controls in their general support systems and major applications:
    a. General Support Systems
        1) Assign Responsibility for Security.
        2) System Security Plan. Shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35). Security plans shall include:

a) Rules of the System.	b) Training.
c) Personnel Controls.	d) Incident Response Capability.
e) Continuity of Support.	f) Technical Security.
g) System Interconnection.	

3) Review of Security Controls. When significant modifications are made to the system, but at least every three years.
4) Authorize Processing. Use of the system shall be re-authorized at least every three years.

b. Major Applications
1) Assign Responsibility for Security.
2) Application Security Plan. Shall be incorporated into the strategic IRM plan required by the PRA. Application security plans shall include:

a) Application Rules.	b) Specialized Training.
c) Personnel Security.	d) Contingency Planning.
e) Technical Controls.	f) Information Sharing.
g) Public Access Controls.	

3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years.
4) Authorize Processing.

4. Assignment of Responsibilities.

5. Correction of Deficiencies and Reports
a. Agencies shall correct deficiencies which are identified through the reviews.
b. **Reports on Deficiencies**. In accordance with OMB Circular A-123, material deficiencies shall be included in the annual FMFIA report. Less significant deficiencies shall be reported and progress on corrective actions tracked at the agency level.
c. Summaries of Security Plans. Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the Paperwork Reduction Act.

3. GISRA (Government Information Security Reform Act of 2000)
FISMA replaced GISRA.

4. CSA (Computer Security Act of 1987)
FISMA repealed CSA.

5. ITMRA (Information Technology Management Reform Act of 1996) / CCA (Clinger-Cohen Act)

ITMRA/CCA assigns the head of each agency the responsibility to assess Information Technology (IT) resources and makes him/her responsible for effectively managing the risks of IT investments. Recent amendments to this CCA included in the Intelligence Reform and Terrorism Prevention Act of 2004 have created mandatory security responsibilities for the agencies and their CIO.

a. Requires an inventory of all computer equipment under agency's control; and maintenance of an inventory of any such equipment that is excess or surplus property.
b. Includes security as a requirement for systems planning and acquisition by agencies.
c. Provides OMB greater authority in guiding agencies on information security issues, with some specific exemptions.
d. Codifies the Chief Information Officer responsibility for the security of the information technology architecture.

6. OMB Circular A-11, Preparation, Submission, and Execution of the Budget
OMB A-11 provides guidance to agencies on how to prepare annual budget submissions. Part 1 provides an overview of the budget process. Part 2 covers development of the President's Budget and describes how to prepare and submit materials required for OMB and Presidential review of agency requests and for formulation of the FY 2007 Budget, including development and submission of performance budgets for FY 2007. The performance budget replaces the annual performance plan required by the Government Performance and Results Act.

a. Submit a Report on Information Technology to OMB (OMB Circular A-11, Exhibit 53). Per Exhibit 53, agencies are required to have major IT investments within 10% of cost, schedule, and performance objectives.
b. Submit an OMB Circular A-11 Exhibit 300 for each major IT system. Exhibit 300 requires information on plans and justifications for major acquisitions as identified in OMB Circular A-11, Section 300: Any information technology system reported as a major system in Exhibit 53 (Parts 1, 2, 3, and 4) must also be reported on Exhibit 300;
c. Ensure information and systems are secure and that security is part of the management of the process from initial concept and throughout the entire life cycle of the investment. Agencies must also protect privacy in a manner consistent with relevant laws and OMB policies, including privacy impact assessments where appropriate.

7. FMFIA (Federal Managers Financial Integrity Act of 1982) (31 U.S.C. 3512 et seq.)
FMFIA requires agencies to establish and maintain internal control. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations and audits should be coordinated and considered to support management's assertion about the effectiveness of internal control over operations, financial reporting, and compliance with laws and regulations.

Evaluate and report annually on the control and security of financial systems contained within each agency.

Amendment to the Accounting and Auditing Act to require ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control.
(d)(2) OMB shall establish guidelines for the evaluation by agencies of their systems of internal accounting and administrative control to determine such systems' compliance with requirements.
(3) By December 31 of each year, the head of each executive agency shall prepare a statement –
(A) that the agency's systems of internal accounting and administrative control fully comply with the requirements; or
(B) that such systems do not fully comply with such requirements.
(4) …include a report in which any material weaknesses in the agency's systems of internal accounting and administrative control are identified and the plans and schedule for correcting any such weakness are described.

8. OMB Circular A-123, Management's Responsibility for Internal Control

OMB Circular A-123 provides guidance to agencies and Federal Managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control to meet the requirements of the Federal Managers' Financial Integrity Act (FMFIA) of 1982, OMB revised internal controls in Section II to better align with current standards.

a. Identifies security as a necessary component to all internal controls. Specifically, "the safeguarding of assets is a subset of all of those objectives." Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of assets;
b. Requires a separate section (Section III) and a listing of statutes for agencies to consider when assessing internal control; and
c. Introduces a new assurance statement on the effectiveness of internal control over financial reporting, which will be a subset of the overall FMFIA assurance statement.

9. OMB Circular A-127, Financial Management Systems

OMB A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.

10. FFMIA (Federal Financial Management Improvement Act of 1996) (31 U.S.C. 3512)

FFMIA requires agencies to have financial management systems that substantially comply with the Federal financial management systems requirements, standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the U.S. Standard General Ledger (SGL) at the transaction level. Financial management systems shall have general

and application controls in place in order to support management decisions by providing timely and reliable data.

a. Develop and implement general and application controls compliant with guidance provided by FASAB and SGL;
b. Make a determination annually about whether the agency's financial management systems substantially comply with FFMIA; and
c. Develop a remediation plan if systems are found to be non-compliant with FFMIA, and determine whether the deficiencies must be reported pursuant to FMFIA.

11. PRA (Paperwork Reduction Act)
Amended by GPEA.

12. GPEA (Government Paperwork Elimination Act)
GPEA enacted to make government service delivery more efficient while ensuring baseline standards for electronic signatures across federal agencies.

Perform business case analysis, cost/benefit analyses, technology assessments, and risk assessments to determine which technologies, systems, and procedures best support compliance with GPEA.

13. GPRA (Government Performance and Results Act)
GPRA requires strategic plans and goals to be integrated into: (i) the budget process; (ii) the operational management of agencies and programs; and (iii) accountability reporting to the public on performance results, and on the integrity, efficiency, and effectiveness with which they are achieved. The primary purpose is to assess program effectiveness and improve program performance.

Develop strategic plans, set performance goals, and report annually on actual performance compared to the goals relating to agency budget, operational management, and reporting to the public on performance results

National Institute of Standards and Technology

14. **800-16** Information Technology Security Training Requirements: A Role and Performance-Based Model
15. **800-18** Guide for Developing Security Plans for Information Technology Systems
16. **800-23** Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
17. **800-26** Self-Assessment Guide for Information Technology Systems
18. **800-30** Risk Management Guide for Information Technology Systems

19. **800-34** Contingency Planning Guide for Information Technology Systems
20. **800-37** Guide for the Security Certification and Accreditation of Federal Information Systems
21. **800-47** Security Guide for Interconnecting Information Technology Systems
22. **800-50** Building an Information Technology Security Awareness and Training Program
23. **800-53** Recommended Security Controls for Federal Information Systems
24. **800-55** Security Metrics Guide for Information Technology Systems
25. **800-60** Guide for Mapping Types of Information and Information Systems to Security Categories
26. **800-61** Computer Security Incident Handling Guide
27. **800-64** Security Considerations in the Information System Development Life Cycle
28. **800-65** Integrating Security into the Capital Planning and Investment Control Process